



RESOLUTION R-017-23

A RESOLUTION OF THE WALKER COUNTY BOARD OF COMMISSIONERS TO ADOPT AN EMPLOYEE ELECTRONIC PROPERTY AND COMMUNICATIONS SYSTEM POLICY

WHEREAS, the Board of Commissioners of Walker County (“Board”) is the governing authority of Walker County, Georgia; and

WHEREAS, the Board has determined it is desirable and necessary to update the county’s Employee Electronic Property and Communications System Policy to clarify the responsibility of each employee concerning the use of county computers and networks; and

THEREFORE BE IT RESOLVED by the Board of Commissioners of Walker County, Georgia that the Walker County Government Employee Electronic Property and Communications System Policy, attached hereto marked “Exhibit A,” and incorporated by reference, is hereby adopted and shall be implemented immediately.

BE IT FURTHER RESOLVED any other Resolution or county policy addressing the use of county computer and network systems prior to this date, that is now in conflict with any of the provisions of this Resolution, is hereby repealed.

SO RESOLVED this 23rd day of March, 2023.

ATTEST:

WALKER COUNTY, GEORGIA

Whitney Summey
Whitney Summey Deputy Clerk

Shannon K. Whitfield
SHANNON K. WHITFIELD, Chairman



The foregoing Resolution received a motion for Passage from Commissioner Askew, second by Commissioner Blackmore, and upon the question the vote is 3 ayes, 1 nays to adopt the Resolution.

**ELECTRONIC PROPERTY AND COMMUNICATION SYSTEMS POLICY****Statement of Policy**

The County provides a variety of channels for communication to promote the efficient operation of its business. All communications transmitted by, received from, or stored in these systems are the sole property of Walker County and an employee should have no expectation of privacy related thereto. All electronic communication systems, supplies, equipment, computers, disk drives, information, and any other material or electronic County property obtained and used during the course of employment (regardless whether during normal working or non-working hours) is exclusively owned by Walker County.

Monitoring of Electronic Communication Systems

IT system monitoring will take place where appropriate, and investigations will be conducted when reasonable suspicion exists of a breach of this or any other policy. Periodic monitoring of activity on County systems, including internet and email use, is appropriate to ensure security and effective operation, and to protect against misuse.

Any electronic communication system usage may be monitored at any time at the discretion of the Human Resource Director along with the Information System/Technology Director. These situations should be restricted to internal investigations or official investigations, such as for law enforcement proceedings. Their staff may be involved as needed and at the determination of the Human Resources Director and the Information System/Technology Director. Any monitoring exercises will exclude involvement by Managers, Directors, Elected Officials and their staff. The Human Resources Director will report findings to the Board of Commissioners.

The Information System/Technology Director is authorized to oversee and manage all County communication systems. To facilitate that role, the Information System/Technology Director may create additional and detailed policies consistent with this Policy, which policies shall be complied with by employees upon distribution of the same. A copy of any such policies promulgated by the Information System/Technology Director shall be maintained in the Human Resources Department. The Information System/Technology Director shall immediately notify reported suspected violations of this policy to the Human Resources Director.

The burden of responsibility is on the employee to abide by this Policy and, prior to use, inquire about specific uses not cited. It is the employee's responsibility to report suspected breaches of security policy without delay to your Department Head, the IT department, or an Elected Official. All breaches of information security policies will be investigated. For any and all questions on topics not covered, please inquire with your supervisor or the Information Systems and Technology Department.

Mobile Phones

County cellular phones/smartphone devices are provided to key individuals for the purpose of ensuring accessibility and enhancing individual efficiencies in handling County business. Cellular phones are not a personal benefit and are not intended for use as a primary mode of personal communication.

Excessive use of a personal cellular device while on County duty may result in disciplinary action. Department Directors have the authority to restrict or prohibit the use of any mobile device, County supplied or personal, at any time, while an employee is on the job if it is determined that use of a mobile device presents a safety hazard or distracts from the duties of the job.

Specifics on Computer and Network Usage**a) Responsible Use of Resources**

You are responsible for knowing what information resources (including networks) are available, remembering that the members of the community share them, and refraining from all acts that waste or prevent others from using these resources or from using them in whatever ways have been proscribed by the Walker County Board of Commissioners and the laws of the state and federal government.



ELECTRONIC PROPERTY AND COMMUNICATION SYSTEMS POLICY

b) Use of Computer Devices

You are responsible, in coordination with your Department Director, for the security and integrity of Walker County information stored on your computer devices. This responsibility includes making regular disk backups and controlling physical and network access to the machine. Avoid storing passwords or other information that can be used to gain access to other government computing resources.

c) Access to Facilities and Information

1) Sharing of Access

Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. You are responsible for any use of your account.

2) Permitting Unauthorized Access

You may not install or otherwise configure software or hardware to intentionally allow access by unauthorized users.

3) Use of Privileged Access

Special access to information or other special computing privileges are to be used in performance of official duties only. Information that you obtain through special privileges is to be treated as private.

4) Attempts to Circumvent Security

Users are prohibited from attempting to circumvent or subvert any system's security measures. This section does not prohibit use of security tools by system administration personnel.

5) Decoding Access Control Information

You are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

6) Denial of Service

Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized personnel of resources or access to any Walker County computer system or network are prohibited.

7) Harmful Activities

The following harmful activities are prohibited: creating or propagating viruses; disrupting services; damaging files; intentional destruction of or damage to equipment, software or data belonging to Walker County Board of Commissioners or other users; and the like.

8) Unauthorized Monitoring

You may not use computing resources for unauthorized monitoring of electronic communications.

9) Government Dishonesty

You should always use computer resources in accordance with high ethical standards and in correspondence with local, state and federal law.

10) Use of Copyrighted Information and Materials

You are prohibited from using, inspecting, copying, and storing copyrighted computer programs and other materials, in violation of copyright laws.

11) Use of Licensed Software

No software may be installed, copied, or used on Walker County resources except as permitted by the owner of the software. Software subject to licensing must be properly licensed and all licensed provisions (installation, use, copying, number of simultaneous users, term of license, etc.) must be strictly adhered to. Any and all new software installations must be approved in some form by the County's designated network and computing personnel.

12) Political Campaigning; Commercial Advertising

The use of system materials, supplies, equipment, machinery, or vehicles in political campaigns is forbidden. Political campaigns and commercial advertisements shall not be displayed on government property. The use of County computers and networks shall conform to these policies.

13) Personal Business

Computing facilities, services, and networks may not be used in connection with compensated outside work or for the benefit of organizations not related to the business of the County. Any other incidental use (such as electronic communications or storing data on single-user machines) must not interfere with other users' access to resources (computer cycles, network bandwidth, disk



ELECTRONIC PROPERTY AND COMMUNICATION SYSTEMS POLICY

space, printers, etc.). State law restricts the use of state facilities for personal gain or benefit.

Internet and Email Conditions of Use

All employees will be assigned an internet access usage level by their Constitutional Officer/Department Head when hired. Use of Walker County Government internet and email is intended for business use. Personal use of the internet or email is permitted where such use does not affect the individual's business performance, is not detrimental to Walker County Government in any way, is not in breach of any term and condition of employment and does not place the individual or Walker County Government in breach of statutory or other legal obligations. All individuals are accountable for their actions on the internet and email systems.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorized access or loss of information, Walker County Government enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Case must be taken to not leave confidential material on printers or photocopiers. All business-related printed matter must be disposed of using confidential waste bins or shredders.

Working Off-Site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with Walker County Government remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car (exceptions for law enforcement maps apply).
- Laptops must be carried as hand luggage when traveling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care must be taken with the use of mobile devices such as laptops, mobile phones, smartphones, and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs, and removable hard drives must be only used in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Walker County Government authorizes mobile storage devices with encryption enabled should be used when transferring sensitive or confidential data. Failure to comply with these provisions will result in disciplinary action up to and including termination.

Software

Employees must use only software that is authorized by Walker County Government on Walker County Government computers. Authorized software must be used in accordance with the software supplier's licensing agreement. All software on Walker County Government computers must be approved and installed in the Walker County Government IT Department.

Viruses

The IT department has implemented centralized, automated virus detection and virus software updates within the Walker County Government. All PCs have antivirus software installed to detect and remove any virus automatically. Individuals should not attempt to remove or disable the anti-virus software.



ELECTRONIC PROPERTY AND COMMUNICATION SYSTEMS POLICY

Telephone (Voice) Equipment Conditions of Use

Use of Walker County Government voice equipment is intended for business use. Individuals must not use Walker County Government equipment for sending or receiving private communications on personal matters, make hoax or threatening calls or accept reverse charge calls for personal reasons from domestic or International operators. All non-urgent personal communications should be made at an individual's own expense using alternative means of communication.

Actions upon Termination

All Walker County Government equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Walker County Government at termination of employment. All Walker County Government data or intellectual property developed or gained during the period of employment remains the property of Walker County Government and must not be retained beyond termination or reused for any other purpose.

When you cease being a member of the government community, or if you are assigned a new position and/or responsibilities within the County, your access authorization must be reviewed. You must not use facilities, accounts, access codes, privileges, or information for which you are not authorized in your new circumstances.

Failure to comply with the provisions within this policy will result in disciplinary action up to and including termination.